Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 38 (2012) 2329 – 2336

Procedia Engineering

www.elsevier.com/locate/procedia

International conference on modeling optimisation and computing-(ICMOC-2012)
April 10&11, 2012

A Survey on DoS Attacks and Detection Schemes in Wireless Mesh Networks

Ms.Sanam E Anto[a] , Ms. S Seetha[b], Robin K Kuriakose[a], a*

[a]*P.G Scholar, Department of Information Technology, Karunya University, Coimbatore, TamilNadu, India*
[b]*Assistant Professor, Department of Information Technology, Karunya University, Coimbatore, TamilNadu, India*

Abstract

A Wireless mesh network is a dynamically self-organized, self-configured, multi-hop wireless network. The WMNs provides wireless services for a variety of applications in personal, local, campus and metropolitan areas. The important application scenarios provided by WMNs includes broadband home networking, community and neighborhood networking, enterprise networking, transport systems, building automation, health and medical systems, security surveillance systems etc. The open nature, dynamic topology and distributed nature of the WMNs makes the network vulnerable to various types of attacks. Of all the types of attacks, the denial of service attack poses the greatest threat and it is very difficult to prevent. In this paper various methods have been proposed for countering the denial of service attacks in wireless mesh networks.

Keywords: WMNs; Denial of service attacks; Flooding; selective forwarding attacks

1. Introduction

Wireless mesh networks are the emerging multi-hop wireless networks which provide a cost-effective solution to extend the coverage of the existing wireless networks. WMN is a special type of adhoc network which has emerged as a key technology for the next generation wireless networking. WMN is

* Tel.:+91-957-800-2831
E-mail address: sanamantoe@gmail.com.

doi:10.1016/j.proeng.2012.06.278

mainly used by the Internet Service Providers for offering Internet connectivity to the users. The architectural components of a WMN include mesh clients, mesh routers and gateways [5]. Mesh routers form the wireless backbone which provides services to the mesh clients by relaying packets to and from the Internet. WMNs have one or more mesh gateways which provide backhaul connectivity to the Internet. Nodes in a WMN have the capability of dynamic self-organization and self- configuration with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves. These attributes provide WMNs with many advantages such as reliability, scalability and low upfront cost. Due to these properties, WMNs have found their applications in various scenarios such as Broadband home networking, Community and neighbourhood networking, Transportation systems, Building automation, Health and medical systems etc.

Based on the functionality of the nodes, the architecture of the WMNs can be classified in to infrastructure/backbone WMNs, client WMNs and hybrid WMNs. In infrastructure/backbone WMNs, the mesh routers form an infrastructure for the clients that connect to them. In client WMNs, the client meshing provides peer-to-peer networks among client devices. In this architecture, the client nodes constitute the actual network to perform routing and configuration functionalities and provide end user applications to customers. Hybrid WMN is a combination of infrastructure and client meshing. In hybrid WMNs, mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients.

Since WMNs are used for various applications, the security in wireless mesh network is a serious concern to be addressed. Various kinds of attacks that affects the wireless mesh networks includes wormhole attacks, resource depletion attacks etc. A major attack occurring in a wireless mesh network is the denial of service attack. Denial of service attacks will make the server overloaded with many requests which will make the server unable to service the requests from the legitimate users. Sometimes the Dos attack will be occurred from multiple agents from multiple locations which is known as a DDos attack

The rest of the paper is organized as follows. Section II discusses about the security requirements of wireless mesh networks. Section III explains about the denial of service attacks in various layers of wireless mesh networks. Section IV discusses about various methods proposed for countering the denial of service attacks in wireless mesh networks. Section V concludes the paper by discussing about various advantages and disadvantages of the methods that is used for countering the denial of service attacks.

2. Security requirements of wireless mesh networks

The main features of a secure wireless mesh networks [15] includes confidentiality, integrity, availability, authenticity, non-repudiation, Authorization and Anonymity. Confidentiality ensures that certain informations are accessible only to the authorized users. Confidentiality is maintained by keeping the data secret from all the entities which do not have the privilege to access the data. Integrity ensures that the messages that are being transmitted from the sender to receiver is not altered or corrupted. It ensures the correctness of the message. Malicious altering and accidental altering of the messages compromises the integrity of the message. The survivability of network resources is ensured by the availability. Denial of service is a major threat to the availability of resources. Authenticity ensures that the participants who are included in the communication are genuine and not impersonators. Without authentication, the adversary can impersonate a benign entity and can gain access to the confidential resources. In order to ensure that the sender or receiver of a message cannot deny the sending or receiving of the message, non-repudiation is used.

3. Denial of service attacks in wireless mesh networks

A denial of service attack makes a computer or network resource unavailable for its intended users. It includes the combined efforts of a person or a group of persons to prevent the service from functioning

efficiently, temporarily or indefinitely. Denial of service attack [9] makes the server or the victim overloaded with huge number of requests, so that the server won't be able to service the legitimate user's requests. A DoS attack is said to occur in a wireless network, if the authorized users are not provided a requested service within a defined maximum waiting time. It is the most dangerous attack which can be launched on any layer of wireless mesh networks.

Mesh Routers are the skeletal backbone of wireless mesh networks and in order to protect it, a high level of security is needed. A malicious attacker can easily inject a denial of service attack into the wireless mesh networks, since it run in the unlicensed 2.4GHZ band. The main aim of DoS attack is to deplete the network resources by sending a flood of packets from one or more compromised nodes including mesh clients and mesh routers. A DoS attack will cause congestion in the network by injecting huge amount of traffic into the network.

An attacker will launch the DoS attack by generating the spoofed source address thereby posing a serious threat to the wireless mesh networks. Also the characteristics of wireless mesh networks make it more vulnerable to DoS attacks. The communication between the network devices or a single device from sending or receiving targeting availability is prevented by the DoS attacks. Availability ensures that only the authorized users are allowed to access the data, services and the network resources from anywhere anytime.

4. DoS attacks in various layers of wireless mesh networks

4.1 Physical layer

Jamming [10] is the most important attack is the most important attack affected by the physical layer. The jamming attack obstructs the legitimate communication. The unlicensed 2.4GHz frequency band is used by WMN's at the physical layer. A radio jamming device or a source noise will make the physical layer unavailable. Radio analyzers are mainly used for detecting these attacks. Since the radio analyzers require very special hardware, the implementation of radio analyzers will be difficult. In a wireless mesh network, the jamming attacks can be launched from anywhere in the mesh network. Selective jamming attacks can be mainly of two types namely, Channel-Selective Jamming and Data-Selective Jamming.

4.2 Link layer

A shared medium is used by the wireless mesh network MAC. So it is highly vulnerable to selfish attack and collisions. The selfish attacks will help in improving bandwidth, throughput and QoS of the selfish node at the cost of another node. RTS\CTS is compromised for the MAC layer DoS attack either by sending bulk of MAC control messages to an innocent neighbor or by holding the MAC channel for unnecessary continues transmission keeping an innocent node back-off. Also de-authentication attack[11] is found in the link layer of WMNs

4.3 Network layer

The network layer of WMNs is highly vulnerable to different DoS attacks. The DoS attacks in the network layer degrade the network performance by exhausting network resources. Black hole attack is a type of DoS attack in which the malicious node absorbs all the traffic going towards the target node. Grey hole attacks is in which, the malicious node selectively forwards the packet to the destination node. The Wormhole[12] attack is another type of DoS attack is in which the attacker in a network records the bits at one location, tunnels them selectively to another location and retransmits them into the network.

Flooding attack is in which the attacker transmits a flood of packets towards a target node or to congest the network and degrades its performance.

4.4 Transport layer

The transport layer DoS attacks includes SYN flooding attacks and the de-synchronization attacks. The SYN flooding attack denies the legitimate service access. It is a TCP-targeted DoS attack. In this attack, the attacker creates a large number of half-opened TCP connections with a victim node but it never completes the handshake to fully open the connection. In de-synchronization attack, a malicious node desynchronizes an authenticated mobile node from the base station, forcing the mobile node to re-authenticate itself. A stronger de-synchronization will allow an attacker to permanently desynchronize the node so that it can never re-authenticate itself.

5. Detecting denial of service attacks in wireless mesh networks

Sudip Misra, P. Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, S.Fredun[1] proposes the DLSR(A DDoS preventing optimized link state routing protocol) protocol which initially detect the DoS attacks , takes necessary actions to minimize the number of service requests to the server coming from the attacking hosts, thereby preventing the DoS attacks. They developed a system model in which each mesh node employs learning automata for the detection and removal of malicious packets passing through it. The functioning of DLSR protocol mainly includes 3 phases. They are,

i) DDoS detection
ii)Attack Identification
iii)The DDos defense phase

DDoS detection phase is performed by assigning a maximum service capacity to the server. The service capacity of a server can be defined as the maximum number of requests a server can process at a unit time. Also a service threshold which is a percentage of the service capacity is assigned to a server. A DDoS attack is identified when the number of service requests exceeds the maximum service capacity or the service threshold that is assigned to the server. The server monitors all the incoming packets. Once a DDoS attack is detected, a DALERT packet is send to all the nodes by the server in order to make them aware that a DDoS attack is detected. Once a DALERT packet is send, all the nodes will enter into an attack identification phase.

After the DALERT packet is send to the nodes, the nodes will enter into an attack identification phase. The nodes will get the server's IP address from the DALERT packet. At this moment, the nodes won't be having any idea about the attacker's information's. The nodes will sample all the incoming traffic and will make a note of all the hosts who are trying to request services from the server. If a host is trying to request many number of services , the node will identify that host as an attacker host. The information about this attacker host is then send to other nodes using an attackers information packet, AIP. If more number of hosts are trying to request many number of services, the details of that hosts will also be send to the nodes using AIP. Once an AIP is received by the nodes, they will enter into the DDos defense phase.

The nodes enter into a DDoS defense phase after receiving an AIP packet. In this phase, the nodes sample the incoming traffic and it will discard all the packets which come from the identified attacker hosts. While continuing to monitor the traffic, if any hosts are found to be an attacker, again the AIP

packets including the information about the attackers are send to the nodes. Thus by discarding the identified malicious packets, the load on the server can be reduced thereby preventing the DDoS attacks.

The advantage of the proposed protocol is that it is able to detect and prevent the DoS attacks in a wireless mesh network. The disadvantage includes that since sampling of packets is done in each node, the energy will be consumed and latency will occur in the network. Also the protocol will consider all the nodes sending a bulk amount of packets as an attacker node. Even if a legitimate user sends a large amount of packets, that node will be considered as an attacker node.

Devu Manikantan Shila, Yu Cheng, Tricha Anjali[2] proposes an effective algorithm called channel aware detection algorithm to detect and locate the selective forwarding attackers [14] in the wireless mesh networks. The CAD algorithm utilizes the methodologies of channel estimation and upstream/downstream traffic monitoring to discriminate the selective dropping attack from the estimated normal loss rates. Two procedures used by the CAD algorithm is channel estimation and traffic monitoring. In channel estimation, the normal loss rate due to the bad channel quality or medium access collision is estimated. In traffic monitoring the actual loss rate is monitored and if the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes will be identified as attackers. Also upstream and downstream monitoring is done.

The channel estimation procedure sets an upstream detection threshold and downstream detection threshold. The behaviour of the neighbouring node is judged by comparing the upstream/downstream observations against the detection thresholds to identify the misbehaving nodes. In order to maintain the detection accuracy during the changes in the network status, the threshold will be dynamically adjusted. The advantages of this approach are that CAD detects the attackers efficiently and increases the packet delivery ratio of the network. The algorithm is a light weight algorithm for multi-hop networks and it utilizes both upstream and downstream traffic monitoring for improved performance. The disadvantage includes: CAD algorithm is not so efficient in detecting an attack when the attacker introduces noise to simulate a noisy channel which affects the sensing process leading to inaccurate threshold.

Lakshmi Santhanam, Deepti Nandiraju, Nagesh Nandiraju, Dharma P. Agrawal[3] proposed a cache based defense at the MRs for identifying flooding style DoS attacks. Most frequently used cache mechanisms are used to identify such flows and an alert is raised to curb them. The paper mainly addresses the problem of combating DoS attacks by raising an early alert. A simple method that maintains minimal state information is employed at each router which functions independently of the underlying queuing mechanism at the router. Two components are employed at each router. They are active DoS attack detection module and DoS attack regulator module.

The active DoS attack detection module identifies the high bandwidth attack flow based on MFU cache discipline. The DoS attack regulator module [7] employs a trace notifier that applies limits along the upstream router through which the attack flow passes. The proposed scheme is implemented above the MAC layer and no changes are required in the MAC firmware of the routers. The cache based defense mechanism regulates the traffic rate of the incessant flows. The misbehaving flows are pre-empted from the IFQ of the MRs by dropping them. The advantages of the scheme is that it offers an active line of defense against DoS attacks. Performance degradation is averted by dropping the identified attack flows along the forwarding routers. The DoS attacker regulator module will effectively control the high rate attack flow. The attacker regulator module moderates the buffer occupancy of the attack traffic and ensures a fair allocation of the link bandwidth. The disadvantage is that the cache based scheme regulates only those flows that are generating excessive UDP traffic.

Biswa Ranjan Swain, Bibhudatta Saboo[4] proposed a probabilistic model for mitigating Denial of service attack and to save the computational time. The number of packets examined is based on the probabilistic approach, not based on the hop count. The probabilistic approach is mainly used to reduce the computational time and memory during the processing of a packet. The probabilistic approach is implemented at the server side. In the hop count filtering method [6], the hop count is indirectly stored in

the TTL field of the IP header. The attacker cannot falsify the hop count of the packets since it is determined by the Internet routing infrastructure. So it is difficult for an attacker to weaken the routers to alter the values of packets that are going through them. The algorithm for hop count filtering method extract the

Table 1. . Comparison of detection and prevention techniques

Authors	*Method*	*Scheme*	*Description*	*Environment*	*Advantages*	*Disadvantages*
Sudip Misra, P.Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, S.Fredun,	DLSR protocol	Detection &Prevention	The protocol helps to detect and prevent the DoS attacks.	Simulation in ns3	i)Detects and prevents Denial of service attacks in wireless mesh networks	i) Due to the sampling of packets in each node, latency will occur.
D.M. Shila, Yu Cheng, and T. Anjali	CAD Algorithm	Detection	The algorithm detects and locates the selective forwarding attacks.	Simulation in ns2	i) Efficient detection of the attackers and improved packet delivery ratio.	i) It is difficult to detect the attacks, when noise is introduced into the channel.
Lakshmi Santhanam, Deepthi nandiraju, Nagesh Nandhiraju,Dharma P.Agarwal,	Cache based defense	Detection	The mechanism identifies the flooding style DoS attacks.	Simulation in ns2	i)Effectively controls the high rate attack flow.	i) Regulates only the flows that are generating excessive UDP traffic.
Biswa Ranjan Swain, Bibhudatta Sahoo,	Probabilistic method	Prevention	The probabistic model helps to mitigate the denial of service attacks.	Simulation in ns2	i)Overhead is less since all the packets are not checked.	i) Instead of dropping all the erroneous packets, only 80-85% of the packets are dropped.

.

final TTL and the IP address. The initial TTL is also assigned. The hop count is then computed by subtracting the initial TTL from the final TTL. The stored hop count is got by indexing the IP address. If the stored hop count and the computed hop count is equal, the packet is a legitimate packet. Otherwise the packet is a spoofed packet.

A probabilistic approach is used in order to find out the number of malicious packets among a huge number of packets. Consider that the number of packets arrives at the server with a Poisson's distribution

λ. The probability that a packet arriving at the server to be malicious is 'p' and to be non-malicious is '1-p'. The number of packets to be malicious can be computed as,

$$P\{N1 = n\} = \sum_{m=0}^{\infty} P\{N1 = n, N2 = m\}$$

$$==e^{-\lambda p}(\lambda p^n/n!$$

The advantage of the scheme is that the overhead is less since all the packets are not checked and the disadvantage of the scheme is that instead of dropping all the erroneous packets, only 80-85% of the packets are dropped.

6. Conclusion

The paper mainly discusses about the security requirements of wireless mesh networks, the major security attack called denial of service attack and different detection and prevention methods for avoiding the denial of service attacks in wireless mesh networks. The first paper [1] proposed a protocol known as DLSR protocol for detecting and preventing the Dos attacks. The scheme was helpful in detecting and preventing the DoS attacks. But the disadvantage of the scheme was that whichever hosts send a bulk amount of request, that host will be identified as an attacker, even if it is a legitimate user. The second paper [2] discusses about the channel aware detection algorithm which can be used for mitigating the selective forwarding attack which is a type of denial of service attack. In order to improve the performance, CAD uses both upstream and downstream monitoring. The disadvantage of the scheme is that if the attacker introduces noise into the network, it is very difficult to identify and prevent the attack. The paper [3] proposes a cache based defense for preventing the flooding style DoS attacks at the mesh routers. It is an active level of defense against the DoS attacks. It will also help in controlling the high rate of traffic flow. The disadvantage is that the scheme regulates only the rate of UDP traffic flow. The paper [4] proposes a probabilistic approach for finding the probability of the number of malicious packets in order to mitigate the denial of service attack. The disadvantage is that only 80-85% of the malicious or erroneous packets are dropped using this scheme.

References

[1] Sudip Misra, P.Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, S.Fredun,"An adaptive learning routing protocol for the prevention of Distributed denial of service attacks in Wireless mesh networks," Computers and Mathematics with Applications,2010, pp. 294–306.

[2] D.M. Shila, Yu Cheng, and T. Anjali. "Mitigating selective forwarding attacks with a channel-aware approach in wmns" Wireless Communications, IEEE Transactions on, 9(5):1661 –1675, May 2010

[3] Lakshmi Santhanam, Deepthi nandiraju, Nagesh Nandhiraju,Dharma P.Agarwal, "Active cache based defense against DoS attacks inWireless mesh networks", pp.419–424.

[4] Biswa Ranjan Swain, Bibhudatta Sahoo, "Mitigating DDoS and Saving Computational Time Using a Probabilstic approach and HCF method," 2009 IEEE International advance computing conference(IACC 2009) Patiala, India, pp. 1170–1172, March 2009.

[5] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE communication. Mag., vol. 43, no. 9, pp. S23-S30, Sept. 2005.

[6] Jin, C.Wang, H. Shin, Kang G. "Hop-Count Filtering: An Effective Defense Against Spoofed Traffic", IEEE Transactions on Dependable and Secure Computing, 2004.

[7] N.B. Salem, J. P Hubaux, "Securing wireless wesh networks,"IEEE Wireless Communications,13(2), pp.15-55, April 2006.

[8] N. S. Nandhiraju, D. Nandhiraju, L. Santhanam, and D.P. Agrawal," A cache based traffic regulator for improving performance in IEEE 802.11s based mesh networks networks," in the Proc. Of the RWC,2000

[9] Seth S, Gankotiya A, "Denial of Service Attacks and Detection Methods in Wireless Mesh Networks,"Recent Trends in Information, Telecommunication and Computing(ITC),pp.238-240,March 2010.

[10] Alejandro Proano and Loukas Lazos,"Selective Jamming attacks in Wireless networks," In proceedings of the IEEE International Conference on Communication,2010.

[11] Rupinder cheema, Divya Bansa, Dr. Sanjeev Sofat,"Deauthentication/Disassociation Attack:Implementation and Security in Wireless Mesh Networks", International Journal of Computer Application,vol 23-no.7,june 2011.

[12] Muthukkumarasamy, Portmann,"Detecting Man-in-the Middle and Worm hole attacks in Wireless Mesh Networks",Advanced Information networking and applications,pp.530-538,May2009.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. International Conference on Mobile Computing and Networking, Boston, MA, 2000.

[14] D. Manikantan Shila and T. Anjali, "Defending selective forwarding attacks in mesh networks," in Proc. 2008 Electro/Information Technology Conference , Ames, IA, May 2008.

[15] P.Yi, Y.Jiang, Y.Zhang, S.Zhang, Security for mobile adhoc networks, *Acta Electronica Sinica* 33 (5) (2005) 893-899.